Commonwealth of Kentucky
Cabinet for Health and Family Services

Cabinet for Health and Family Services (CHFS) Information Technology (IT) Policy

065.014 Cabinet for Health and Family Services (CHFS) System Development Life Cycle (SDLC) and New Application Development

Version 2.2
April 27, 2017

Revision History

Date	Version	Description	Author
7/20/2010	1.0	Effective Date	CHFS OATS Policy Charter Team
4/27/2017	2.2	Revision Date	CHFS OATS Policy Charter Team
4/27/2017	2.2	Review Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
CHFS Chief Information Officer (or designee)	4/27/2017	ROBERT E PUTT	
CHFS Chief Security Officer (or designee)	4/27/2017	DENNIS E. LEBER	

Table of Contents

1 065.014 Cabinet for Health and Family Services (CHFS) System Development Life Cycle (SDLC) and New Application Development

Category: 065.000 Application Development

1.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must establish an acceptable level of security controls to be implemented through a system development lifecycle. This document establishes the Cabinet's System Development Life Cycle (SDLC) and New Application Development Policy which helps manage risks and provides guidelines for security best practices regarding projects, systems, web servers, or web applications to ensure quality development projects are delivered on time, compliant at the state and federal level, and within budget.

1.2 Scope

The scope of this policy applies to all internal CHFS employees, consultants, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer, application, and data communication systems. External vendors providing information security or technology services may work with the CHFS agency(s) for exceptions to this policy.

1.3 Roles and Responsibilities

1.3.1 OATS Information Security Team

Responsible for the assessment, planning, and implementation of all security standards, practices, and commitments required. This team is responsible for the adherence of the CHFS SLDC and New Application Development Policy.

1.3.2 Privacy Lead

The individual(s) responsible for providing security and privacy guidance for protection of Personally Identifiable Information (PII), Electronic Personal Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff and contractor personnel. This role is responsible for the adherence of the CHFS SDLC and New Application Development Policy in concert with the OATS Information Security (IS) Team.

1.3.3 CHFS Staff and Contract Employees

Individual(s) must adhere to the CHFS SLDC and New Application Development Policy as well as referenced documents that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system.

1.4 Management Commitment

This policy has been approved by OATS Division Directors, CHFS Chief Technical Officials, and CHFS Chief Information Officer (CIO). Senior Management supports the objective put into place by this policy.

1.5 Coordination among Organizational Entities

OATS coordinates with other organizations or agencies within the cabinet with access to applications or systems. All organizational entities that interact with CHFS systems, within or contracted with OATS, are subject to follow requirements outlined within this policy.

1.6 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in though state laws and regulations as well as federal guidelines outline in the National Institute of Standards and Technology (NIST). Applicable agencies additionally follow security and privacy framework outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

2 Policy Requirements

2.1 General

This policy is established to refine uniform business processes and standards to assure quality development projects are delivered on time and within budget.

Each system or group of related systems will define a methodology for managing Software Development Life Cycle (SDLC). The methodology will consist of an Initiation, Development, Testing, User Acceptance testing (UAT), as required, Implementation, Maintenance and Operations (M&O), and Decommissioning phases. Information Technology (IT) needs and work should be coordinated through or with the Office of Administration and Technology Services (OATS).

CHFS projects shall use the TFS, or agency other approved system(s), to check code in and out during development or for use in production when required. The IS Team recommends that the code be digitally-signed to maintain integrity between development, integration, test, and production environments.

Each system or group of systems will have an oversight group who will have the responsibility of managing projects and changes in accordance with the SDLC methodology. The oversight group will consist of designated members of the OATS project team, the responsible OATS branch manager, designated members of the applicable business unit(s) as prescribed by the business sponsor, and members of the OATS executive team. The responsibilities of this oversight group will include tasks such as review, approval, denial, and referral of requests. The leader of the oversight group will be the OATS branch manager or a designee.

Agencies will be responsible for identifying critical systems based on the nature of the data and the system's business function or mission. The term "critical system" refers to the server, or servers, that support one or more critical business application. This may include web servers, database servers, and other servers that are essential to the operation of the business application. Per Enterprise Policy- CIO-082 Critical Systems Vulnerability Assessments Policy, each agency shall engage a third party to assess all critical systems under the agency's responsibility both upon initial implementation into production use and at least every two (2) years thereafter.

These network and server vulnerability assessments do not include the development environments, or application software, related to these systems, which must be tested separately. Each agency shall follow the appropriate notification process outlined in this policy prior to conducting these assessments. It is the responsibility of the agency, in consultation with the Cabinet CIO, to engage an appropriate and qualified organization that is considered an external or third party entity to ensure objectivity and accuracy in the assessment.

2.2 Definitions

- Application – A software program designed to perform a specific function (e.g., Partner Portal, Benefind, etc.).
- Application Server – A component-based product that resides in the middle-tier of a server centric architecture (e.g., IBM WebSphere).
- Database (server or components) – A database management system (DBMS) is a computer software application that interacts with the user, other applications, and the database itself to capture and analyze data. A general-purpose DBMS is designed to allow the definition, creation, querying, update, and administration of databases.
- Oversight Group- CHFS comprised group including agency and technical staff that will be a part of communication and movement throughout the SDLC process.

- Web Server - A computer that runs a Web site. Using the HTTP protocol, the Web server delivers Web pages to browsers as well as other data files to Web-based applications (e.g., Internet Information Server (IIS), or Apache).

2.3 SDLC Steps

2.3.1 Initiation

- A mechanism for submitting requests for system software changes or enhancements must be formalized by each oversight group.
- Requests must be reviewed by designated members of the OATS project team to ensure that sufficient information is available and a tracking number is assigned and logged.
- Requirements must be gathered and documentation of the details of the business needs and objectives will be completed.
- Requests will be prioritized, estimated hours for requirements, development, and testing will be determined and a proposed release will be assigned.
- The documented business requirements and the corresponding system specifications documents reflecting the changes needed to the system, will be reviewed with representatives of the business unit (s) and final approval will be obtained.
- Proposed releases will be reviewed with members of the oversight group in regularly scheduled meetings to be conducted at least once a month.

2.3.2 Development

- Upon approval of written system specifications by the representatives of the business unit(s), modifications to systems will be made to reflect the changes specified.
- System development will occur during the specified release window.
- The appropriate development team will document the system modifications to module(s) impacted by the system specifications.
- The appropriate development team will complete unit testing prior to the code being turned over to the appropriate OATS IS or Testing team.

2.3.3 Security Scanning, Assessments, and Testing

- All major software changes in a specific release will be validated and approved for production by the appropriate OATS IS or Testing team.
- Testing will consist of system testing, regression testing, and test plan/script execution, as required.
- If applicable UAT will be conducted by designated members of the business unit.
- All system issues identified during testing shall be logged, prioritized, and appropriate defects shall be corrected by development staff and retested within the targeted release.
- All applications will undergo compliance testing for Americans with Disability Act (ADA) compliance. CHFS will follow the W3C WCAG 2.0 Level AA standard to

ensure this majority test is completed for all internal and external applications within CHFS.

- The status of the release will be reviewed with the oversight group and a “Go/No Go” or a delayed status will be determined during regularly scheduled meetings.

2.3.4 Implementation

- The validated software changes shall be authorized by OATS branch manager or designee to be moved to the production environment.
- The oversight group will be advised of the move and an effective date and time of the release to production.
- The oversight group will be provided with a notification identifying all system modifications for the release.
- Post implementation reviews will be conducted with OATS project team as needed.

2.3.5 Maintenance and Operations

- In the M&O Phase, the IT solution's system components, data, and infrastructure are maintained in the production environment and monitored to ensure they continue to meet business needs.

2.3.6 Decommissioning

- When the system is no longer used or needed decommission the system is a crucial step to ensure errors are reduced, cost is reduced, and to help minimize unnecessary activities from occurring. An inactive system or application must be decommissioned to reduce the vulnerabilities and threats that could occur.
- Agency management, or designees, must identify the application elements and date to decommission. This plan and all details must be shared with the OATS IS or Testing Team.

2.3.7 Exception

- At times an accelerated SDLC is required due to the urgency of a system fix. If an emergency fix is required, system specifications document documenting the requested change will be completed by designated members of the OATS project team and is to be immediately approved by an OATS management staff member. Once approved the system change request is provided to the assigned developer.
- Upon completion, the development team will turn over the modification to the OATS IS Team and if applicable for UAT. Upon sign-off by the OATS IS Team and/or the business unit testing team, final approval will be obtained from a representative of the business unit. The modified software changes will then be implemented into the production environment as soon as feasible.

2.4 New Application development

OATS requires all new application development efforts to be reviewed and analyzed. All new application development efforts must follow the outlined steps below:

2.4.1 Step 1

New application development must be submitted to the IT Technical Architecture group for analysis and approval of the technical architecture of the solution. Submissions must be in accordance with the CHFS IT Standard 2400- Database Management Software Standard.

2.4.2 Step 2

The data owner or assigned designee must sign-off on the vision, scope, and optional functional requirements that are documented.

2.4.3 Step 3

The OATS IS Team or an approved contractor must perform a security assessment on the new application, per the CHFS 020.205 IT System Technical Assessment Policy.

2.4.4 Step 4

The new application must undergo UAT, CHFS SDLC steps, and receive the approved agency sign off before deployment into production.

3 Policy Maintenance Responsibility

The OATS IS Team is responsible for the maintenance of this policy.

4 Exceptions

Any exceptions to this policy must follow the procedures established in CHFS OATS Policy: 070.203.

5 Policy Review Cycle

This policy is annually reviewed and revised on an as needed basis.

6 References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS OATS Policies List
- CHFS OATS Standards List
- CHFS OATS Policy: 020.205- IT System Technical Assessments Policy
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Controls Policy
- CHFS OATS Standard: 2400- Database Management Software Standard
- Commonwealth of Technology (COT) Enterprise IT Policies;
- COT Enterprise Architecture and Kentucky Information Technology Standards

(KITS) Library;

- COT ITSC Exception/Addition/Modification Request Form;
- Enterprise IT Policy: CIO-082- Critical Systems Vulnerability Assessments Policy
- Enterprise Security Exemption Request, COT-F085
- Health Insurance Portability and Accountability Act of 1996 (HIPAA):
- HIPAA Security Rule § 164.308 (1)(ii)(A)(B);
- Internal Revenue Services (IRS) Publications 1075
- National institute of Standards and Technology (NIST) Special Publication 800-18 Guide for Developing Security Plans for Federal Information Systems
- National institute of Standards and Technology (NIST) Special Publication 800-30, Rev. 1, Guide for Conducting Risk Assessments;
- National institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- National institute of Standards and Technology (NIST) Special Publication 800-66, Rev. 1, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule;
- Social Security Administration (SSA) Security Information